299_Spiccioli-di-Cassandra--Una-sturiellett-come-soluzione-al-Datagate-

Spiccioli di Cassandra/ Una sturiellett come soluzione al Datagate?

(299) - Ricordi di mailing list, quando c'era chi tentava di convincere gli iscritti a cifrare le proprie comunicazioni. Esperimento…

Spiccioli di Cassandra/ Una sturiellett come soluzione al Datagate?
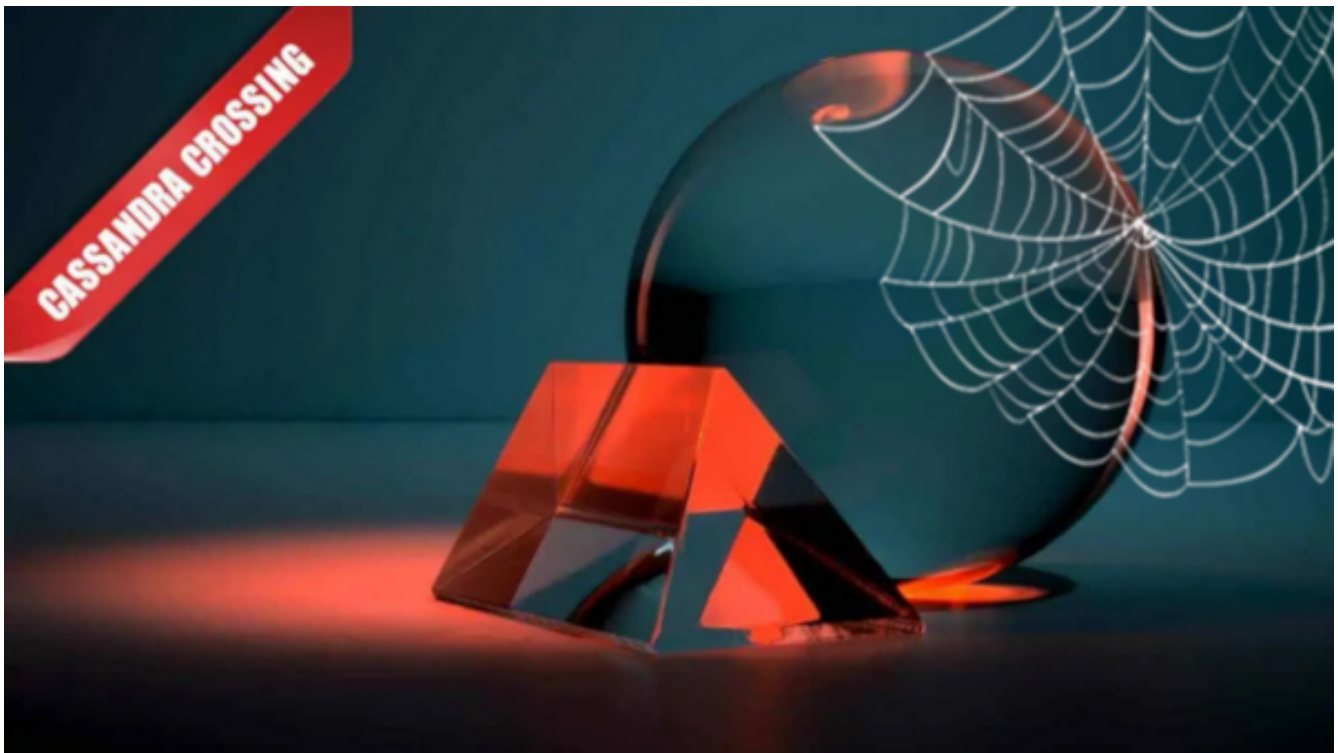
Figure 1:

(299) - Ricordi di mailing list, quando c'era chi tentava di convincere gli iscritti a cifrare le proprie comunicazioni. Esperimento fallito, ma varrebbe la pena di ritentare.

Roma—Successe in un agosto dello scorso millennio, nemmeno ricordo l'anno esatto, e neppure accurate ricerche nei miei archivi di posta sono riusciti a determinarlo.

Fu una piccola piccolezza della storia delle maillist italiane, che alcuni protagonisti ricordano molto bene.

Il luogo fu una "titolata" maillist dell'epoca, ben frequentata dalla meglio gioventù dei guru italiani della Rete. Alcuni di essi tenevano i keynote speech in convegni negli States, o davano contributi titanici ai maggiori progetti di software libero dell'epoca come Debian. Malgrado la loro indubbia competenza e provata "fede", tuttavia, non prestavano la minima attenzione a firmare e/o crittografare le loro mail, con le solite motivazioni del "dovrei ma non ho tempo" o del "tanto a chi vuoi che gliene freghi qualcosa di quello che scrivo".

Cassandra, non ancora nata ma già considerata una talebana della privacy, era sfiduciata e sfinita da un numero immane di discussioni bi o multilaterali sulla necessità di usare Pgp/GnuPG per tutte le comunicazioni via mail al fine di rafforzare il web-of-trust e rendere impraticabili intercettazioni "mirate".

Concetto semplice, noto, condiviso: tutti d'accordo ma nessuno lo faceva.

Non ricordo se la paternità dell'idea sia stata di Cassandra, di Settembre-san o semplicemente fu una supercazzola nata per generazione spontanea durante uno dei nostri scambi privati di mail. Fatto sta che, ambedue frustrati da questo problema, in quattro e quattr'otto mettemmo su una piccola sceneggiatura per una scambio di mail farlocche e provocatorie sul tema.

Iniziando con un'innocua mail sull'argomento, prevedeva un crescendo artificiale di mail sempre più acide ed incazzate, un vero e proprio flame, in cui uno dei faceva il poliziotto buono e l'altro quello cattivo, e che attirò come una calamita molte altre persone, proprio quelle che provavano qualche "senso di colpa" sull'argomento.

La cosa fu poi lasciata esaurirsi, ma il risultato netto fu che almeno una dozzina di persone appartenenti alle suddette categorie si generarono le chiavi, configurarono i client di posta (operazione non banalissima all'epoca) e cominciarono ad usare Pgp per firmare digitalmente sempre le proprie mail pubbliche, e per crittografarle quando possibile nella posta privata.

Come tutte le storie a lieto fine la cosa non è durata molto, e non si è diffusa: nemmeno i pochi convertiti sono rimasti tutti saldi sull'attitudine di criptare appena possibile.

Hanno cambiato idea? Probabilmente no. Si sono lasciati nuovamente vincere dalla pigrizia? Forse sì, ma anche no, chissà?

Sono stati inglobati dall'onda delle comunità sociali, che apparentemente rende inutili questi accorgimenti? Probabile.

Eppure, malgrado il lungo tempo trascorso, l'avvento di Facebook e le intercettazioni globali dell'NSA, l'idea di base è più attuale che mai. Usare gli strumenti di crittografia forte, da Pgp a Tor, per tutti coloro che non limitano la propria vita in Rete alle sole comunità sociali, resta un semplice ma efficace mezzo per rendere non intercettabili almeno una parte di quello che viene oggi intercettato.

Si badi bene, rendere non intercettabili i contenuti lascia scoperte ad esempio le reti di relazioni, non risolve la questione, e nemmeno una parte significativa di essa.

Funzionerebbe però benissimo per evitare che l'uso di tali strumenti sia così raro da rappresentare di per sé un motivo sufficiente (e lo è ahimè in maniera anche troppo dimostrata, sia al di qua che al di là dell'oceano) per giustificare il ricorso a tappeto ad "attenzioni" analogiche convenzionali, invasive, e tra l'altro inutili e lesive.

Se un numero rilevante di persone già allora avesse configurato il proprio client di posta, ed anche quello della zia, per scambiarsi ricette crittografate sulle torte di mele, il Grande Fratello del Datagate non ne sarebbe stato granché scalfito, ma certamente questi sillogismi strumentali sarebbero diventati poco o punto praticabili.

Discorso identico vale per l'uso di partizioni criptate, di programmi di wiping del disco, di settaggi per la privacy nei browser, per l'uso di Tor…Non risolvono i problemi del Datagate, ma rendono più praticabile e meno "eversivo" il fatto di prendere quel minimo di contromisure disponibili per mantenere riservato un angolo del proprio sé digitale.

Ricordate la persecuzione di Aaron che non riguardava (almeno direttamente) la privacy od il Datagate, ma si è concretata con le maniere forti usate contro un innocente? Aaron non era solo, ma si era esposto molto, era nel mirino, ed il supporto ricevuto dalla sua Rete non è bastato.

Contribuite affinché il "chi non ha niente da nascondere non ha niente da temere" non diventi nuovamente un enunciato così largamente condiviso da essere "politically correct".

Per farla breve, visto che siamo tutti intercettati, rendiamo la cosa un po' più difficile. Più siamo e meglio stiamo, recita un vecchio adagio.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on April 5, 2023.

Canonical link

Exported from Medium on August 18, 2025.